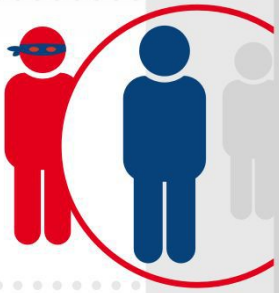
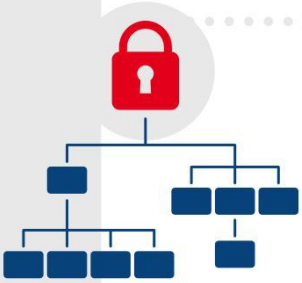
Security Missteps Your Company Should Probably Correct

Companies today have to stay vigilant and aware of all the different methods criminals use to steal from a company. Whether it's to gain access to proprietary company secrets or a more traditional type of theft, there are various techniques used to infiltrate companies in the modern age. Use these ideas to keep your company prepared and prevent stolen property.

#1 Understanding the True Threats for Employees

Many companies fail to realize that their employees and suppliers are at risk of being approached by someone who wants information or money from a company. A cutting-edge security plan is needed to protect your employees from external threats. Your employees should also be trained and versed in what to do in these situations.





#2 Data Security is a Business Issue

Many companies think of data security as an issue for the IT department to sort out. While you can hire an IT company to secure your company, you need to make it a primary concern in your business.

Every decision needs to include a discussion of potential security risks that could result as a consequence online or through your network.

#3 Relying Too Much on Commercial Security Solutions

Your antivirus program isn't enough to completely protect all aspects of your business. While it is important to have an antivirus solution, but this won't stop all threats. You'll need to have a department that actively monitors your network and sets policies to prevent employees from putting the company at risk. Make sure you have ready-made systems in place as well a support system to keep it going.

#4 The Real Threat of Social Engineering

Where many companies fail is when it comes to protecting themselves from social engineering schemes. There needs to be a system in place where all visitors to your site are required to provide the right identification and proof that they are authorized to be on company property.

This includes repairmen and other service individuals. Many social engineering schemes will use several people to ask seemingly innocent questions about the company. With enough information, these people can later come back and gain access to otherwise secure areas.

#5 Not Classifying Trade Secrets

When you don't classify your trade secrets, you are leaving your company open to theft and scandal. It's also important to take control of the growing trend of bringing your own device to work. Employees who bring their own devices put the company at risk by taking private documents home with them, or introducing viruses into the network. Use your company equipment solely for work and regularly service this equipment.

It's important to take control of your business and prevent these issues from costing you a lot of money. By setting up a proper security plan, you can avoid most mistakes and ensure that your company doesn't fall victim to theft. Employ the right people and continue to educate your employees to prevent theft of your company secrets.

Colocation America®
It's All About Connections...®

colocationAmerica.com